A Survey of Group Key Management Protocols in Wireless Mobile

Umi Salma B.
Research Scholar/CS
Bharathiar University

Dr.A.Arul Lawrence
Professor & Head/CS
RGIT, Bangalore

Abstract -- Key management is equally important as compared to any other security measure such as encryption and authentication. With the growing usage of mobile devices and the advent of multicast communication, there has been a significant amount of work carried out in developing an optimum group key management protocol for mobile multicast systems. Key management is widely being adopted in securing group communication for both wired and wireless networks. Securing group communication over wired networks is fairly well established; however, wireless networks bring additional challenges due to member mobility and increase in the number of members. This paper presents a comprehensive survey of group key management protocols in wireless mobile environments that employ multicast communication. They are classified into network dependent and independent protocols and further categorized into tree-based and cluster-based key management protocols. The survey clearly outlines the characteristics of each protocol along with highlighting their advantages and limitations with respect to real-world systems. The paper is concluded with a taxonomy of the individual protocols with respect to the defined requirements which provides a strong source of literature reference for researchers in this field.

Keywords: Mobile Multicast, Security, Group key management, Wireless Network

1. INTRODUCTION TO MULTICAST AND GROUP COMMUNICATION

After the successful testing of Audio cast at the 1992 Internet Engineering Task Force (IETF) the idea of incorporating multicast features in network products has been highly attractive to many vendors. Progress has been slow since initial deployment, especially compared to the likes of the World Wide Web (WWW) and the Hypertext Transfer Protocol (HTTP). The reason for this is because multicast features require additional intelligence in the network which introduces nontrivial amounts of state and complexity in both core and edge routers. However, multicast communication is becoming increasingly important and is a subject of great research interest. We explain the differences between multicast, broadcast and unicast. We also demonstrate the advantages that multicast offers for enabling group communication.

1.1 Unicast vs Multicast

Multicast can be defined as, an inter network function that allows data to be delivered to a specific group of nodes (or recipients) by a single transmission. From a data sender point of view, multicasting allows data to be sent from the source (which is the sender) only once, and the network will make copies of data and transmit the data to multiple destinations (which are known as the recipients of the multicast data) which have been determined prior to transmission. This special feature enables data to be efficiently sent to a group of recipients, and is therefore attractive for group-based application services such as video conferencing, as well as data delivery services such as stock quote, news or weather updates. Multicast is much more efficient than traditional unicast methods, which only transmit data to one intended recipient. We illustrate an example of unicast versus multicast data communication in Figure 18. The left figure shows unicast data communication, while the right figure shows multicast data communication. From Figure 18, unicast and multicast data transmissions are indicated with bold arrows. Based on one -to-many relationship (see Section 18), it shows a single sender (S) sending data to a group of receivers (R).

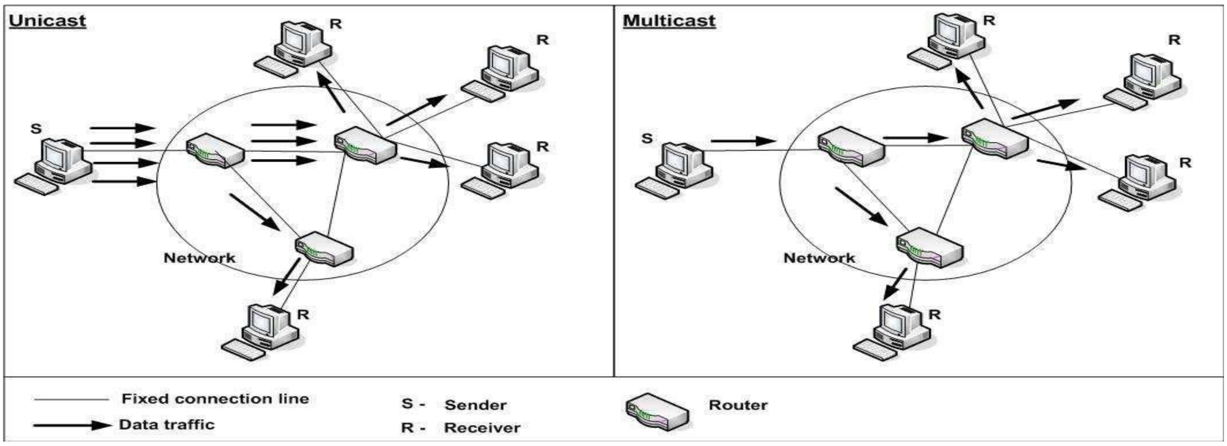


Figure 18: An example of unicast vs. multicast communication

Members needs to be sent across the network separately. Thus, in order to transmit to n recipients (group members); n pieces of data need to be transmitted. As illustrated on the right however, multicast allows a sender of data to transmit only one copy of the data to n recipients. This is achieved when a router (with a built-in multicast function at the network level) makes copies of the data and transmits it to the intended recipients via the nearest routers. End routers (closest to the recipients) will then complete the transmission, and send the data to the intended recipients.

2.1.1 Multicast vs Broadcast

A closely related concept to multicast is broadcast. Commonly used in radio and TV transmission, broadcast is easily understood as a way to transmit data or messages to all recipient nodes in a network. Both broadcast and multicast allow data to be transmitted to more than one recipient at a time. However, in regards to group communication, multicast offers a better solution than broadcast in several aspects. Host coverage. Broadcast includes everyone (all hosts) in the network. This is due to its indiscriminate transmission which can be received by anyone having the correct equipment in place. For example: (i) houses with a specific dish can receive satellite channels cast by a satellite station. (ii) Computers connected to an Ethernet can receive messages cast by the network.

On the other hand, multicast data is not sent to all hosts, but is rather targeted to a predetermined group of hosts which have specific network addresses.

• Internet Protocol (IP) context. Broadcast is usually designated by a single address assigned to all stations in the network (such as an Ethernet packet with a MAC address that can be received by all stations). On the other hand, multicast offers more restricted access with an IP multicast address designating a certain group of hosts in such a way that any transmission from one host in the group is received by all other hosts within the group. More precisely, data packets can only be processed by multicast group members with a correct multicast address. For this to work, a particular address is reserved for that purpose and is found in the destination address field of the message (see Section 2.2).

• From a recipient's context. With broadcast, all recipients will act upon the received message, whereas with multicast only those recipients that have been configured to respond to the destination address in the message will do so. Thus, multicast saves network resources (such as the CPU time) by allowing only the intended group of recipients to further process the message received.

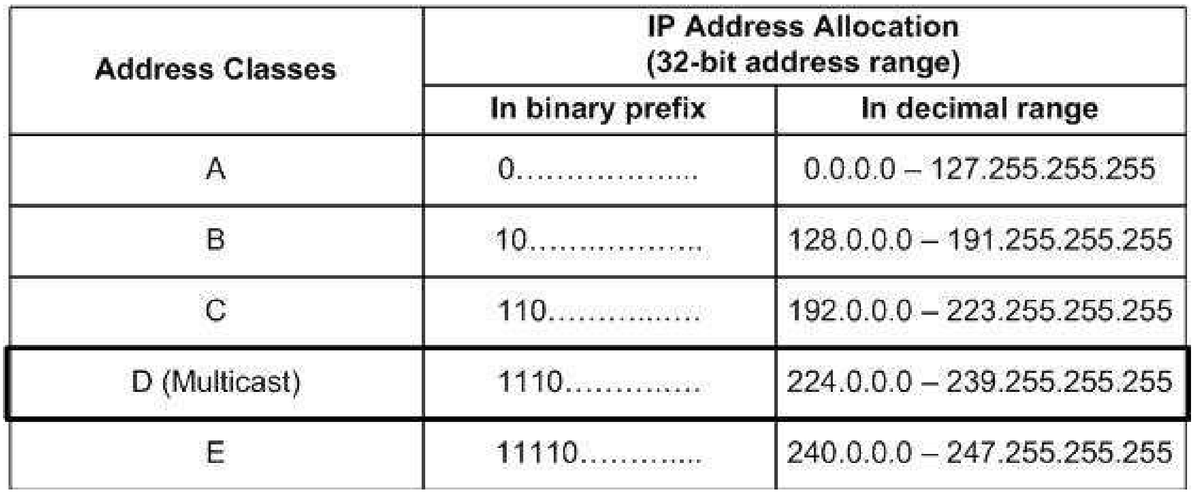
1.1.2 Group Communication vs Multicast Communication

Throughout this thesis, the terms group and multicast group carry the same meaning and will be used interchangeably. We will avoid formal definitions and interchange the terms multicast communication, group communication and multicast group communication. This approach is also supported by the following sources gathered from the American. Heritage Dictionary of the English Language as well as from the Cisco Internetworking Terms and Acronyms (Ammer, 2000) and (Cisco system, 2006), where both terms carry similar meanings, as follows:

Multicast communication (Cisco system 2006) a single communication (like an audio, a video or packets) made and copied by the network and sent across a network to a specific subset of network address. Group communication (Ammer, 2000). A communication that occurs in an assemblage of persons or objects, all interconnected and capable of communicating with each other, in ways that are securely isolated from all other users on the network.

1.2 Multicast Environments

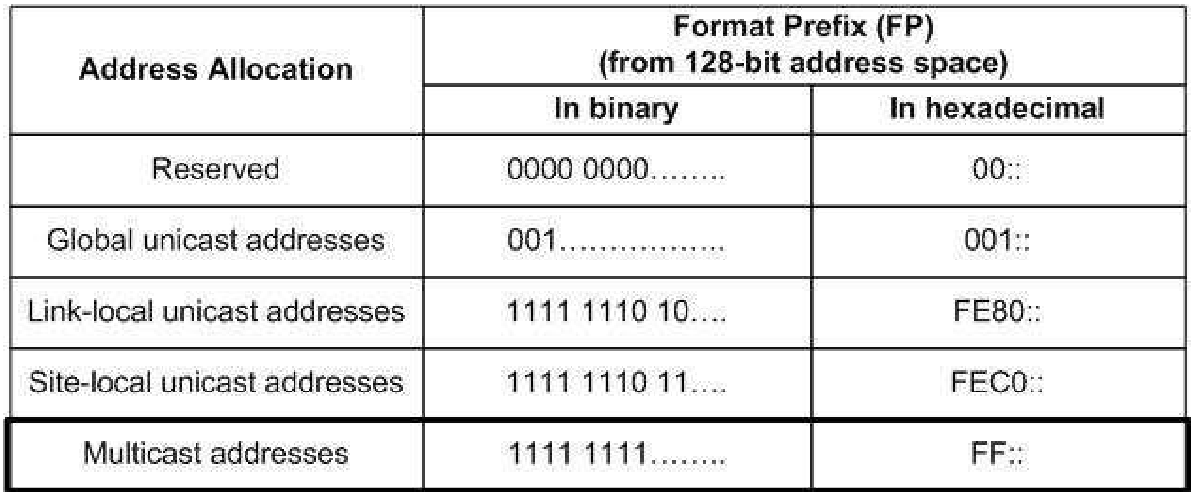
The popularity of multicast has grown considerably with the wide use of the Internet, as well as the increasing demand for group-based applications such as online forums, pay per view channels (PPV), various information dissemination services (such as news, weather, or share prices updates), as well as multimedia conferences including video and audio conferencing. While many internet applications use the conventional point-to-point or unicast transmission, one-to-multipoint or one-to-many transmission was limited to local network applications. The emergence of new applications over recent years has seen changes in the earlier trend of unicast transmission seen as being inadequate to support group-based applications. Thus, multicast transmission is becoming more popular as the demand for these new group applications increases. The original protocol that allowed the transmission of data on the Internet is the Internet Protocol (IP), which supports unicast communication. For multicast to function, an extension was designed to the original IP architecture to incorporate the interesting features of multicast. This extension is known as IP multicast. IP multicast is defined as a transmission of an IP datagram to a group of hosts, identified by a single IP destination address. This address must be one of the special addresses designated for the purpose of multicast communication. We illustrate the allocation of IP multicast addresses in the form of two tables. Table 2.1 gives the allocation of multicast addresses in IPv4 (IP version 4), while Table 2.2 gives the IPv6 (IP version 6) version of multicast address allocation. While an IP multicast group is identified by a class D IPv4 address which ranges from 224.0.0.0 to 239.255.255.255, in IPv6 multicast addresses always begin with 1111 1111 (binary), or FF (hex). This set of addresses can be used for defining different multicast groups (except for several designated addresses which are reserved and will never be used).



Address Classes	IP Address Allocation (32-bit address range)	
	In binary prefix	In decimal range
A	0………………	0.0.0.0 – 127.255.255.255
B	10…………….	128.0.0.0 – 191.255.255.255
C	110……………	192.0.0.0 – 223.255.255.255
D (Multicast)	1110………….	224.0.0.0 – 239.255.255.255
E	11110………..	240.0.0.0 – 247.255.255.255

Table 2.1: Multicast address range in IPv4.

Just like conventional communications that are based on unicast, IP multicast is an unreliable, unordered, and best-effort datagram service. In other words, it does not guarantee that a datagram will arrive at all the destination group nodes, and it is possible that the order of receiving the datagram at the end



Address Allocation	Format Prefix (FP) (from 128-bit address space)	
	In binary	In hexadecimal
Reserved	0000 0000……..	00::
Global unicast addresses	001……………..	001::
Link-local unicast addresses	1111 1110 10….	FE80::
Site-local unicast addresses	1111 1110 11….	FEC0::
Multicast addresses	1111 1111……..	FF::

Table 2.2: Multicast address prefix in IPv6

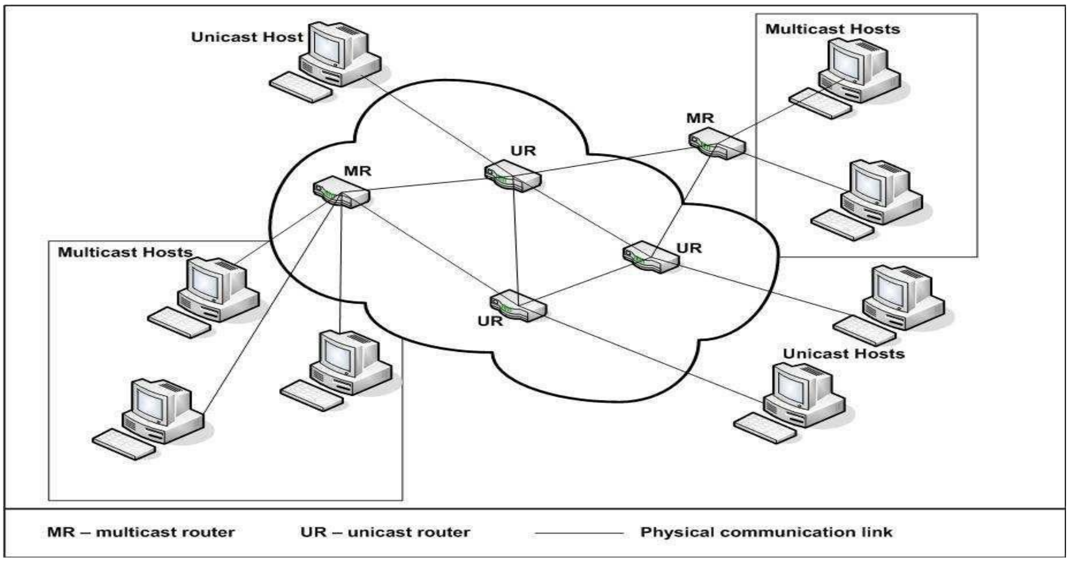
Nodes may change during transmission. In this early age of multicast technology, when multicast functionality has not yet been widely integrated into traditional network routers, an experimental multicast network called multicast bone (MBONE), was constructed as a test bed to realize multicast communication. The original purpose was to carry out the first audiocast of IETF meetings. MBONE is a virtual network consisting of IP tunnels (with virtual point-to-point links) between multicast routers that join the multicast network together. As a consequence, MBONE’s main functional aspect was providing an environment for multimedia conferences for various groups of people from across the Internet.

These tunnels are particularly useful in many conventional unicast networks where many network routers are not multicast capable. For this to work, both end routers (nearest to a group of multicast hosts) need to be multicast capable routers, and IP packets that are addressed to a multicast group are tunnelled between these multicast routers. In practice, the datagram of a multicast group is encapsulated into another IP datagram by the nearest multicast router, and sent across the network through one (or more) unicast routers as unicast datagram’s, which then forward it to the next multicast router of another multicast group. We illustrate a multicast communication over a unicast network in Figure 2.2, with Figure 2.2(a) showing a set of multicast hosts wishing to form a group communication over a unicast network and Figure 2.2(b) depicting the tunnelling of IP datagram’s that occurs between these multicast hosts. Figure 2.2(a) illustrates communication that occurs between several multicast hosts over a traditional unicast network. This is supported by multicast routers (MR) at both ends of multicast hosts. Here, we show that as this communication occurs over a traditional network, the transmission link may have to go through unicast routers (UR) which normally do not support multicast. One way for this to work is by using a technique called tunnelling (see Figure 2.2(b)).

Figure 2.2(b) illustrates two multicast hosts communicating with one another over a unicast network (as shown in Figure 9.2(a)) via a multicast tunnel. This is achieved as follows. When multicast IP datagram's leave the host to the nearest multicast router (MR), encapsulation of multicast packets into unicast IP datagram's is done, before transmitting it over a unicast network with unicast router(s) (UR). At the receiving host, when the datagram's reach the multicast router, the same datagram's will go through a de-capsulation process to recover the original multicast IP datagram's, before being transmitted to the host. This process of encapsulation and de-capsulation creates a multicast tunnel between multicast hosts for enabling multicast communication over a traditional unicast network.

2.3 Multicast Applications

We have now presented an overview of multicast, including the terms that we will use throughout this thesis. We have also demonstrated that multicast technology is more efficient than broadcast and unicast when enabling group communication. In this section, we look at different types of multicast application, as well as several instances of group-based applications that could utilize multicast technology. The main types of multicast application can be divided into two



(a) A set of multicast hosts forming a group communication over a unicast network.

(b) Figure 2.2: An illustration of a multicast communication over a unicast network categories, which are one-to-many and many-to-many relationships

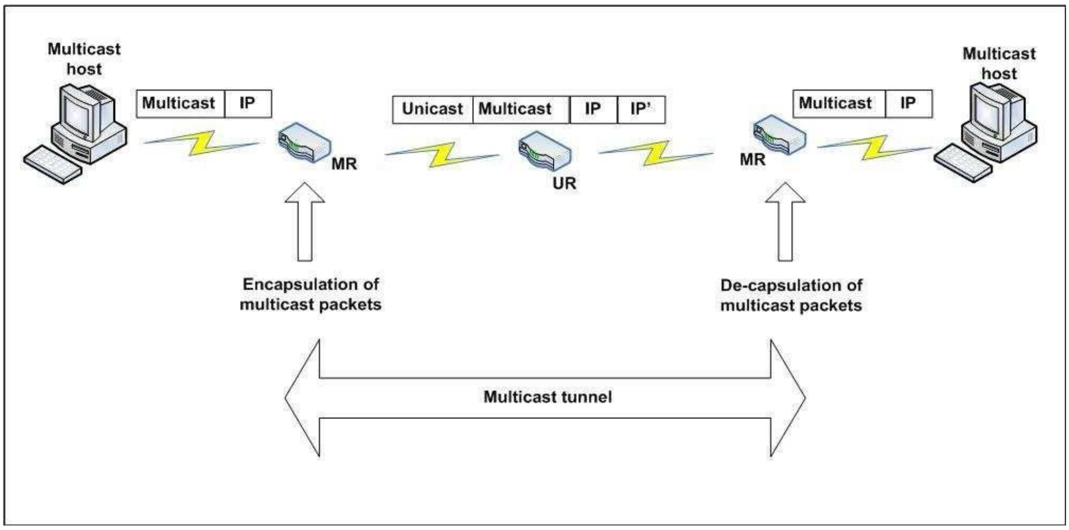


Figure 2.3: A one-to-many multicast (or group-based) communication. Each of these determines the relationship between the sender (S) and the recipients (R) of multicast data.

2.3.1 One-to-Many Relationships

One-to-many relationships correspond to one-Sender to many-Recipients. In this case, there is one entity that is the sender of the group, while one or more entities will be the recipients of the group communication. Figure 2.3 illustrates this type of relationship within a multicast group, where there is one entity that acts as the sole sender of the multicast data, while the others are the recipients.

Amongst the examples of such group communications are the following:

• Data distribution. Push technologies such as stock quote services, weather or news data, updating of sales information or, price list to all branches, as well as advertisement dissemination based on consumer habits or place of residence.

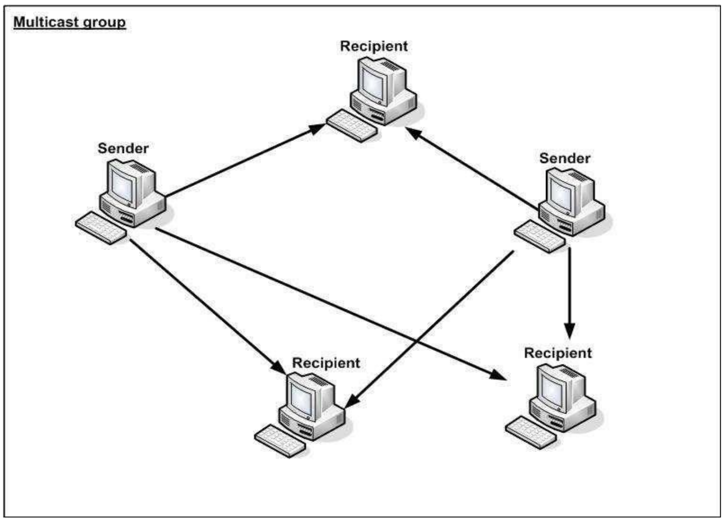
• Streamed data delivery. Widely referred to as broadcasting, such as TV broadcasting as well as Pay per View (PPV) channels. • Software distribution. Software upgrades in a company, as well as the distribution of updates by software manufacturers of their products over the Internet.

2.3.2 Many-to-Many Relationships

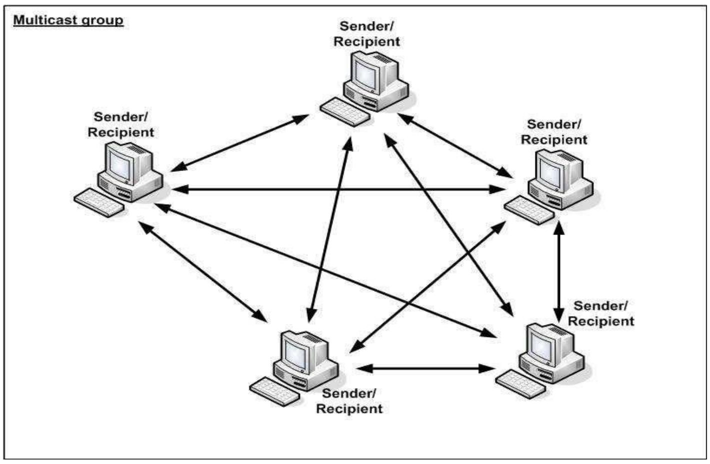
In this type of relationship, many-to-many corresponds to many-Senders to many-Recipients. In this case, there are one or more entities that will be the sender (s) and/or the recipients of the multicast group. Thus, an entity can be a sender, a recipient, or both. Figure 2.4 illustrates this type of multicast application. Figure 2.4(a) shows a multicast group with two entities acting as the senders of data, while Figure 2.4(b) illustrates that every entity within a multicast group can potentially be both the sender and the recipient of data. Among the examples of such group communications are:

• Audio/video and Teleconferencing. Also referred to as Computer-Supported Cooperative Work (CSCW), group members that are located in different sites will share white board tools designed for coordination between members.

• Distance Learning. For example teleteaching, which refers to a scenario in which a student in one place is able to participate in a class somewhere else. This requires group communication between those teaching and those learning, since questions have to be asked and solutions need to be discussed. Another example is virtual classrooms, where course participants use the Internet to obtain teaching materials, deliver their assignments, as well as receive feedback from course instructors. Similarly



(a) With two entities as senders



(b) With every entity can either be the sender, the recipient or both.

Figure 2.4: Many-to-many multicast (or group-based) communications

the instructor distributes papers to the virtual class and assignments are collected from the course participants. Note that some of the above group applications already existed before multicast functionality was designed. These pre-multicast era applications are called applications that emulate group communication. In these applications, very simple group communication mechanisms are implemented in the applications themselves, but not supported by the communication system that underlies them. While this seems to outdate the need for a multicast function, its implementation and performance are very simple. These were literally designed to emulate group communication properties in the application itself. One example is Electronic Mail Systems that allow you to send the same message to groups of recipients, who are normally specified through mailing lists. Other examples are the distribution of news, chatting on the Internet (such as the Internet Relay Chat (IRC)), as well as game servers that allow web users to play games like Backgammon, Chess and Life together on the Internet.

3. SECURITY IN GROUP COMMUNICATION

3.1SECURITY ACTIVITIES AND STANDARDS

This Secure Multicast Research Group (SMuG) was formed to discuss issues related to multicast security, as well as to investigate standards for secure multicast. SMuG's main intentions were to focus on the security problems relating to IP multicast, with the aim of providing common solutions for a variety of applications. The results obtained were presented to the IETF for potential standardization. In order to expand its research scope, SMuG was replaced by The Group Security Research Group (GSEC) (GSEC, 2007), which was another short-lived research group of the IRTF. With GSEC no longer active, the Working Group (WG) that is currently active in research on multicast, as well as group communication security, is known as Multicast Security (MSEC) (MSEC, 2007). Established directly under the IETF organization, MSEC is anticipated to continue the process of standardizing protocols pertaining to security provision of group communications over the global Internet. Three main problem areas have been defined by MSEC as the central research areas concerning secure multicast by IETF (IETF, 2007). They are:

- Multicast data handling. This covers problems pertaining to the treatment of multicast data by the entities involved in the communication, such as encryption algorithms, as well as data integrity techniques.
- Management of keying material. This is concerned with the management of all keying material of a multicast group, including distribution and updating (or re-keying) of all cryptographic keys as well as other security parameters related to the keys (such as information on key expiration periods, or key usage).
- Multicast security policies. This area is concerned with all aspects of multicast group security policies, including creation, translation and representation of policy of a multicast group. It is important that group policy is managed properly since policies may be expressed in different ways, they may exist at different levels and they may be interpreted differently according to the context in which they are specified and implemented. For example, policy negotiation and translation (if necessary) should be performed as part of a host joining a multicast group. Otherwise, it is meaningless as new members will not be able to participate in the group communication due to incorrect or inappropriate policies. Published works in these problem areas can be found in (MSEC, 2007) and (GSEC, 2007). These problem areas are equally important and ought to receive equal treatment in order to accomplish secure group communication. While some genuinely new solutions are required, some of these problems can also be addressed by adapting accomplishments in traditional unicast environments. Our interest in particular concerns with security issues that are specific to multicast group communication. We look at this in the following section.

3.2 SECURITY RESEARCH ISSUES SPECIFIC TO GROUP COMMUNICATION

In this section, we present the main security issues pertaining to group communication. Like unicast, provision of security services for multicast group communications is concerned with confidentiality, integrity, authenticity as well as availability of group communications. As in unicast, an adversary may carry out both passive and active attacks against a multicast communication, such as:

- eavesdropping on confidential communication,
- disrupting a group session,
- blocking data transmission,
- injecting false data traffic,
- masquerading to join a group session,
- initiating a bogus group session, or
- Colluding members exchanging information in order to gain unauthorized access to data which may contain cryptographic key and other group related information. Thus, it is crucial to provide a secure data exchange between group members, which includes use of mechanisms or methods to:

(a) Establish the identity of the originator of a message.
(b) Protect transmitted data, including cryptographic keys, from unauthorized disclosure and modification.
(c) Control group members access to data.
(d) Enable any member to verify the nature of the session in which he participated. With no regard to the order of importance, we address the main issues concerned with the provision of security for group (multicast) communication in the following sections.

3.2.1 Group Membership Policy

Multicast capability of sending data only to a specific group of hosts (group members) requires some additional processing to restrict access to the specific group. This processing includes the management of group membership. The status of group membership of a multicast group is determined by the group membership policy. This is defined during the creation of a multicast group. The policy of group membership can be categorized into two types, as follows:

- Static policy. Often referred to as closed membership, group membership with a static policy offers a restricted approach to allowing hosts to take part in a multicast group. In this case, group membership of a multicast group is predetermined prior to the commencement of a group communication and all group members belong to a certain multicast group throughout its lifetime. For example, a video conferencing facility for a global organization might have a predefined group of hosts corresponding to its multiple branch sites. While no increment in the group size is possible (no new members are allowed to join the group), some Circumstances need to be considered with regards to members leaving the group:

(a) Group members may be permitted to leave during a group session.

(b) Group members may be allowed to re-join (after leaving) the group session, except for cases where group members are deliberately evicted from the group session. (This is a reasonable policy since group members may well leave a group due to a disconnection that is beyond their control.)

- Dynamic policy. Also referred to as open membership, a dynamic policy allows any hosts to join (or leave) a multicast group at any time throughout the lifetime of the multicast group. It is essential to define this group membership policy because it determines the entire set of procedures for a particular multicast group communication.

3.2.2 Key Management

Key management for multicast communication is generally more complex than for unicast environments. In a secure environment, presuming that a request to establish a multicast session among a group of hosts is granted, a common group key needs to be distributed to each of the group members prior to the start of the group session. In secure group communication, specific problems for managing the keying material can be divided into two approaches depending on the group membership policy in place, as follows:

- Static approach. Due to its fixed membership policy, the static approach requires almost no change (or update) in keying material throughout the lifetime of a multicast group except for periodic re-keying (see Section 4.3.2). This implies that a new multicast group will need to be created to cope with new members joining the multicast group.
- Dynamic approach. The dynamic approach, where any hosts can join (and leave) a multicast group at any time, potentially requires that cryptographic keys be updated whenever there is a change in group membership. The precise need for updating the keys is primarily determined by whether the following services are required:

(a) Backward secrecy. This ensures that past communications, including group keys and their related information, are inaccessible to newly joined members. For provision of backward secrecy, group keying material has to be updated whenever a new join to the group occurs.

(b) Forward secrecy. This ensures that future communications remain inaccessible to departed members. For provision of forward secrecy, re-keying of keying material has to occur whenever an existing member leaves the multicast group. One of the main challenges in key management for group communication is the distribution of the keys needed by group members of a multicast group. Dynamic group membership aggravates the complexity of the protocols which handle the distribution of cryptographic keys. In particular, it is important to ensure that each group member gets keys for the right group sessions. Additionally, if backward or forward secrecy is required, it is necessary to deny some group members access to specific cryptographic keys.

3.2 Security Research Issues Specific to Group Communication

3.2.3 Group Security and Authentication

In secure multicast environments, as mentioned in Section 3.2, provision of security services such as entity authentication, data confidentiality and data integrity are required. However, secure multicast group communication has some specific requirements in these areas:

(a)As hosts may wish to join specific groups, and different groups may have their own security requirements (for example, concerning who can join), it is imperative that: • Group managers verify that the service provided by a multicast group is accessible only to authorized group members.

(b)Group members verify that the service they participate in is provided by a genuine source.

- Both (group managers and group members) verify each others identities. (b) Different policies (static or dynamic) may require different needs for managing group keys (due to joins and leaves). In a dynamic policy, if backward and forward secrecy are required then re-keying of group keys will have to occur whenever there is a change in group membership.

3.2.4 Scalability

In general, the term scalability refers to the ability of a framework (or mechanisms within a framework) to be extended to cover a larger group of hosts over a wider physical region without too much delay and deterioration in the level of service provided. In the context of secure group communication, the need for scalability primarily affects the management of keying material. In particular, it affects the choice of types of cryptographic key that are needed for group communication, and the methods by which the keys are updated, keeping in mind that in dynamic environments the size of the group membership may gradually change over time. While the problem of hosts joining seems to be straightforward (if the provision of backward secrecy is not necessary) and distribution of new cryptographic keys can be supported by the old cryptographic keys, group members leaving poses a much more difficult scalability problem. If the provision of forward secrecy is necessary, new keying material must be sent to the remaining group members in a way that excludes the leaving member. One method that can be used is to send the key updates to each group member separately (each of which is protected by an individual key). This creates a scalability problem if the group is large and/or has a very dynamic group membership. Thus, the scalability issues for secure group communication need to be addressed from an early design stage of any key management framework.

4. GROUP KEY MANAGEMENT FRAMEWORKS (GKMF)

This chapter discusses group key management frameworks (GKMF) for multicast group communications. In Section 4.1 we introduce GKMFs. In Section 4.2 we discuss methods that Can be used to design a GKMF. Section 4.3 describes the main components of a GKMF. Section 4.4 discusses security threats that could compromise the multicast group communication security. In Section 4.5 we describe the main GKMF security requirements for group communication. Section 4.6 discusses general aspects of key management. Finally, in Section 4.7, we present the important features necessary for a good GKMF design.

4.1 Introduction

As discussed in Chapter 3, the IETF multicast research group (MSEC) defined three main problem areas pertaining to multicast group communication security. One of these was key management. A group key management framework (GKMF) is an infrastructure comprising the basic entities and functions necessary to provide common cryptographic key(s) to all the members. In particular a GKMF specifies:

- Entities and relationships. The placement of entities involved in group communications and their relationships, as well as determining roles and responsibilities for managing the cryptographic keys necessary for multicast groups.
- Key management processes. The management operations necessary to control the cryptographic keys that are needed for group members to engage securely in group communications. This includes generation, distribution, as well as updating (or re-keying) of keys. These are expressed in terms of the protocols required to support these key management processes. These include protocols for creating multicast groups, registration of group members to multicast groups, as well as distribution of keys to group members.

4.2 Design Approaches

Design approaches for establishing a GKMF can be classified in a number of different ways. One way is to distinguish between static and dynamic key management (see Section 3.2.2). Static approaches clearly have limited application and more commonly dynamic approaches are required. Group key management frameworks can be further distinguished by two design approaches, depending on whether a designated central entity can be relied upon for key management purposes:

(i) Centralized schemes

Centralized schemes require a central entity to govern and manage group keying material. As the main point of security reference, all group members are required to trust this entity. The advantages of adopting centralized schemes are that:

(a) They are easy to manage, since the provision of trust is focused on one entity.

(b) They save some transmission overheads, since authentication of a central entity (such as a group or key manager) may only need to be done once by group members during a multicast group session. On the other hand, centralized schemes share inherent drawbacks as follows:

(a) Bottlenecks may occur if there is implosion of transmissions where group members send messages to the central entity at the same time, and vice versa.

(b) Having a central entity as the only point of reference creates a single point of failure. If the central entity fails then the whole system collapses, which then results in paralysis of the multicast groups in place.

(c) A central entity requires a large capacity for storing keying materials for the entire system.

(ii) Distributed schemes

Distributed schemes avoid the need for a central entity. In these schemes, each member of a multicast group is equally trusted, and all (or a few) members are required to take part in managing the keying material, including generation of cryptographic keys. For example, one method that can be used is that group members who join early generate the keys and then distribute them to others who join the group later.

The advantage of distributed schemes is that they offer more flexibility. On the other hand, drawbacks of these schemes are that:

(a) They do not always scale well, since distribution of management tasks across larger multicast groups can be complex.

(b) In large networks, the messages exchanged between group members can be prohibitively large.

(c) There is always a risk that colluding members may exchange security information.

(iii) Hybrid schemes

Hybrid schemes are a combination of the two earlier approaches (centralized and distributed). These schemes are based on a distributed hierarchy of trusted entities for key management purposes. For example, in a two level hierarchy one or more entities are responsible (at the first-level) for managing sub-entities (at the second-level). A sub-entity at the second level may govern other lower-level entities. From a bottom-up view, lower entities are dependent on the higher-level entities.

These schemes potentially share both the advantages and disadvantages exhibited in centralized and distributed schemes. Since the properties can be fine-tuned using varying levels of hierarchy, the hybrid approach is quite attractive for designing a GKMF.

4.3 Main Components

In this section we look at the main elements that form a GKMF. As mentioned in Section 4.1, these fall into two categories:

4.3.1 Entities and Relationships

The main entities involved in a GKMF are:

• Group members. Group members consist of at least one sender (who sends the data) and at least one recipient (who receives the data).

• Group manager(s). Often referred to as a group controller, key server or key manager, a group manager (GM) controls all group processes, such as registration of group members to a multicast group. In particular, the GM manages the cryptographic keys that are needed for group communication, including the generation and distribution of such keys to group members.

Note that a group manager's role may be performed by separate entities, one of which is responsible for all general activities that concern a multicast group, such as group membership policy, while the other is primarily concerned with security aspects such as group key management.

4.3.2 Key Management Processes

The essential processes identified within a GKMF are described as follows:

• Formation of groups. Formation of a multicast group can be further divided into two processes:

(a) Creation of multicast groups

At the network level, creation of a multicast group can be done by a host sending a request to a network using the Internet Group Management Protocol (IGMP). In return, the network kernel assigns a specific multicast address for the group (see Section 2.2). At this point, all the information related to a multicast group such as group membership policy, as well as the cryptographic keys needed for a group communication, is determined.

(b) Initial registration of group members

Once the interest to join a particular multicast group is determined, a host instructs the network that he wishes to receive data sent to a specific multicast group (at the application level, this is usually indicated by a host requesting a group service on the Internet). When that happens, it is considered that the host joins the group. From another perspective, any host who wishes to join a multicast group sends a join request to a group manager. Presuming that

the host is granted permission to join the group, group related information, in particular the cryptographic keys needed for group communication, is exchanged between the group manager and the group member.

• Generation and distribution of cryptographic keys. Cryptographic keys can be symmetric, asymmetric or a combination of both, depending on the security objectives or preferences of particular multicast applications. Most GKMF proposals use symmetric keys because symmetric algorithms have lower computational complexity and are faster than asymmetric algorithms. Using symmetric cryptography, the main keys needed for a multicast group communication normally consist of:

(a) Individual keys

Often referred to as long-term keys, an individual key is unique for every host (potential group member), and is typically shared with a group manager. Individual keys are generated by a trusted entity in the GKMF (such as a group manager). These keys are usually established prior to the commencement of a multicast group.

(b) Group keys

Often referred to as traffic encryption keys (TEKs), a group key is shared by the group members of a multicast group, and is primarily used for securing the actual data communication. Group keys are also generated by a trusted entity such as a group manager. Group keys are usually distributed to every member of a multicast group under the protection of individual keys. Where asymmetric cryptography is used, all entities involved in the group communication are assigned asymmetric key pairs. Note that apart from the aforementioned keys, an auxiliary key may be needed for the secure and efficient distribution of a group key to group members of multicast groups. Thus, instead of having to send the group key separately under the protection of individual keys of group members, it can be sent once via a multicast message protected under the auxiliary key.

• New member joins. This process is quite similar to initial registration of group members. Any host who wishes to join a multicast group will need to send a join request message to a governing entity such as a GM. If the member is granted permission to join the multicast group then relevant keys need to be delivered to the newly joined member. If backward secrecy is required then it may be necessary to re-key cryptographic keys whenever a new member joins a multicast group. This will result in all group members including the newly joined member obtaining a new group key. Note that new member joins may only be allowed in dynamic policies, since static policies suggest no increment in group members (see Section 3.2.1).

• Existing member leaves. The process of an existing member leaving requires that any member who wishes to leave a multicast group sends a leave request message to a governing entity such as a GM. If forward secrecy is needed then re-keying will need to occur in order to update the group with a new set of group keys unlike members joining, members leaving are considered special because a leave can be:

(a) Voluntary
This type of leave occurs at the request of a group member. A group member may leave a multicast group at any time.
(b)Non-voluntary
This type of leave is not requested by a group member (for example the ejection of a group member). A managing entity such as a group or a key manager is responsible for managing and initiating non-voluntary leaves. Depending on group security requirements, an eviction of a group member (non-voluntary leave) may require re-keying to occur.

- *Re-keying. The process of re-keying group members with new cryptographic keys may occur due to:*

(a) Group membership change
Due to new joins (for backward secrecy), or due to existing member leaves (for forward secrecy). See Section 3.2.2 for more information.
(b) Periodic re-keying.
A pre-determined plan to re-key a multicast group after a certain interval (which is often dictated by a group policy, as well as security requirements of a particular application). This is normally determined prior to the creation of a multicast group.
(c) Expiration of cryptographic keys
When a key has reached the end of its validity period. Often this type of re-keying is synchronized with the periodic re-keying (as in (b)), whichever occurs first?
(d) Compromised keys
When a key used is believed (or suspected) to have been compromised and is no longer considered safe to use. Re-keying events are normally initiated by governing entities such as group or key managers. When re-keying occurs within a group, new keys will be generated and distributed to all group members.

4.4 Security Threats

From the perspective of key management, threats (active or passive threats, or a combination of both) that may compromise the security of multicast group communications may in particular be targeted at data traffic of a group, which includes messages (the actual data communication), and keying materials (the cryptographic keys and related information). In this section, we discuss security threats that could potentially compromise multicast group communication security. They are listed as follows:

- Eavesdropping on group data traffic that contains confidential data or messages as well as keying materials.
- Intercepting data traffic that could result in further malicious use including:

(a) Modifying the contents by inserting part or whole new messages (or parameters) into the group data traffic.
(b) Keeping the contents for further cryptanalysis.
(c) Deleting messages so that the intended member never receives them.

- Recording messages (such as between two targeted group members or key managers) to re-send (replay) at a later time.
- Disrupting or blocking a group session by an adversary (such as flooding the key entities with bogus requests, which could result in denial of service).
- Masquerading as a member to join a multicast group, or to create a bogus session.
- Gaining unauthorized access from exchange of information by colluding members. It is thus important to address these threats when designing a GKMF.

4.5 Main Security Requirements

We have looked at the main components of a GKMF and identified the key management processes and potential security threats in multicast group communications. In this section, we look at the main security requirements which are specific to multicast group communication. Based on existing standard definitions ISO 7498-2 (ISO, 1989), ISO/IEC 11770- 2 (ISO, 1996b), BS ISO/IEC 9798-1 (BS, 1997) and FIPS PUB 199 (FIPS, 2004), we derive the security and trust requirements identified with a GKMF as follows:

- Entity authentication. Both group members and key manager entity(s) need to be able to authenticate and verify each others identities, and by doing so each entity believes that an entity is who it claims to be. This usually occurs via unicast communication between two entities, such as when a host first contacts the key manager to join a multicast group.
- Backward and forward Secrecy. All necessary key materials must be re-keyed whenever there is a change in group membership (either due to new joins or member leaves). While backward secrecy controls access to previous communication from the newly joined members, forward secrecy controls access to future communication from the leaving members.
- Data (Message) integrity and authentication. Both group members and key manager(s) need to be able to check that the data received originates from the claimed entity(s) and that it has not been altered in an unauthorized way. Depending on the level of security of an application, there are two types of checking that can be done, as follows:

(a) Group authentication
All members within a multicast group need to be able to check that a message received originated within the group, and that the message has not been altered by entities outside the group. This type of data authentication is usually useful in multicast communication that occurs between entities who share a common key, such as the real data communication between members of a particular multicast group.
(b) Origin (Source) authentication

Each member (group member or key manager entity) needs to be able to corroborate that the source of data (message) received is as claimed. This type of authentication is often important when one entity needs to verify that the security parameters (keys) received is coming from the claimed entity. For instance, a sub-group key manager will need to be able to corroborate that all messages containing the keys originate from the main key manager.

• Need for trust model. For secure multicast group communication, we need a trust model that includes:

(a) An architecture that is compatible with the existing network protocols.

(b) A framework which is scalable for expansion without affecting too much the level of service and overall system performance.

(c) A trusted managing entity(s) for managing keying material (in particular generation and distribution of cryptographic keys).

•Secure key distribution. All necessary key materials need to be securely distributed to all group members prior to group communication. Secure key updates (re-keying). Key updates must be done securely, since a new set of key materials may need to be distributed whenever a key compromise is suspected, the current keys expire, or whenever there is a change in group membership. Group members need to be Informed by the managing entity(s) whenever there is a change in the key materials that they are using and when key updates are on the way. The re-keying process should be conducted without disrupting any ongoing communication.

4.6 Aspects of Key Management

Secure and proper handling of all aspects of key management is one of the fundamental requirements of any GKMF design in order to form a secure and trusted model for the deployment of group communication. The main aspects of key management are the provision of the following basic key services:

- Key generation. The generation of cryptographic keys for a particular cryptographic algorithm. This needs to be done in a secure and proper manner.
- Key registration. The registration of cryptographic keys with entities. Registration of keys is usually done by a trusted registration authority, and usually applied when symmetric cryptographic techniques are used.
- Key certification. This applies to public key cryptography, to ensure the association of a public key with an entity. Key certification is provided by a certification authority.
- Key distribution. The dissemination of cryptographic keys to the communicating entities. Key distribution can be performed using physical (or manual) techniques, or using a trusted third party such as a key distribution centre (KDC) or a key translation centre (KTC), where keys can be delivered to users by using other keys (often called key encrypting keys)
- Key installation. The installation of a key prior to its use.
- Key update (re-keying). The ending of the use of one key and beginning of use of another key (see Section 4.3.2).
- Key storage. The secure storage of cryptographic keys prior to use, for short-term use, or for back-up. For security reasons, keys are usually stored physically in a secure environment, for instance using tamper resistant hardware. Keys can also be protected by other means, such as by encipherment with other keys, or by controlling access to keys using passwords or PINs.
- Key derivation. A special form of key generation, where a key is derived from other keys using some transformation process. It is important to ensure that compromise of the derived key does not reveal the derivation key or other derived keys.
- Key archiving. The provision of secure long-term storage for keys. Archived keys may be needed at a later time for eneration of new keys or to verify certain claims after the key has expired.
- Key revocation. The revocation of a key after key compromise is suspected, or known, or when it has reached its expiration date. Similar to the process of key update, except that there are no subsequent keys involved.
- Key de-registration. Part of the key disposal process, a key association with an entity is removed. This is done by a key registration authority.

Key disposal. The disposal or destruction of a key that is no longer needed. This process includes all materials (both physical and electronic documents) associated with a key. This should be done in a secure and proper manner so that after the key is disposed, no other remaining information can be used to recover the disposed key. Note that while all of these processes require attention, the majority of GKMFs for group communication are mainly concerned with distribution and updating (re-keying) of cryptographic keys. Other aspects of key management are implicitly assumed to be available and securely managed by trusted entity(s), since their provision is handled by generic key management processes that are not specific to group key environments

4.7 Important Features

We have identified the main entities and processes that form a GKMF. In this section, we identify features that in our opinion a good GKMF should have.

4.7.1 Historic Development

Note that the initial designs of GKMFs considered only the basic features sufficient to support multicast group communication, without considering further needs for security (note that IP multicast was never intended to provide secure multicasting).From the early 1990s we have witnessed the emergence of applications (see Section 2.3) that require secure multicast technology. Thus, the need for secure, reliable and scalable GKMFs has become increasingly important.

Another aspect of this is that, as the demands for group-based applications have increased, service providers have realized that they want more out of the multicast facility. In particular there has been demand to: (a) control access to information to certain groups of hosts.

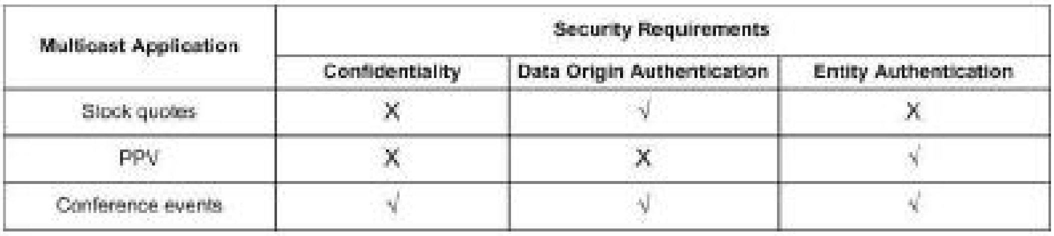
(b) restrict access to valid group members during specific time periods (while they are registered (valid) members of a multicast group).

(c) preclude members who have ceased to be group members of a multicast group.

4.7.2 Different Features for Different Applications

An additional challenge for GKMF design is that different applications typically require different features. There is normally no such thing as one solution fit for all applications, and GKMFs for secure multicast group solutions are no exception. A particular design of a GKMF may be sufficient to meet certain requirements of some multicast group applications, while lacking for others. Consider three applications mentioned in Section 2.3: stock quotes distribution, PPV (Pay per View) channels and conference events.

• Stock quotes. A service providing stock quote information may not require confidentiality (since such data is often public), but the recipients may wish to ensure the integrity of data received and that it originates from a valid sender.



Multicast Application	Security Requirements		
	Confidentiality	Data Origin Authentication	Entity Authentication
Stock quotes	X	√	X
PPV	X	X	√
Conference events	√	√	√

Table 4.1: Multicast applications and their security requirements

• Pay per view. Viewers of PPV channel (the recipients) may not care about source authentication (as long as they obtain the right channels). However, the PPV service providers may wish to restrict access to channels only to users who are actually paying for the service. Note that, due to the nature of application, both viewers and service providers may not require confidentiality services.

• Conference events. Conference events, where only members who have registered for a conference should be granted access to conference materials, may require a confidentiality service. Conference organizers may wish to control access to materials and ensure that only registered members are able to view them. We summarize the security requirements of the aforementioned applications in Table 4.1.

The provision of these different security requirements all involve some kind of cryptographic keys being managed properly and securely within a GKMF, although the precise security services required depend on the requirements of particular multicast applications.

4.7.3 Specification of Features

We attempt here to identify the key features that a GKMF should have. From various studies on existing GKMFs we have extracted the important features of a GKMF and divided them into two parts; essential properties that every GKMF should have and desirable properties that are optional depending on the specific requirements.

4.7.3.1 Essential features

As discussed in Section 4.7.2, different applications may require different properties depending on their specific requirements. We thus classify the essential features that a secure GKMF should have into two further categories:

(1) Independent of application

Independent of application in place, the essential features that a secure GKMF should have are:

• Dynamic group membership policy. To allow a framework to be as flexible as possible group members should be free to join and/or leave any time during any session throughout the multicast group lifetime.

• Backward and forward Secrecy. A good GKMF should ideally provide these on a default basis, maintaining the secrecy of information to valid group members at all times.

• Dynamic and efficient re-keying processes. To efficiently manage any re-keying that will need to occur. Re-keying processes should be conducted without disrupting any on-going communications.

• Scalability. Group communications can potentially involve tens of thousands of members, many of whom may be constantly joining and eaving groups. A GKMF should thus be scalable with respect to the efficient distribution and management of keying material.

• A trust model. A trust model is crucial for a GKMF in order for it to properly function. This should include a security architecture that is compatible with the existing network protocols, as well as scalable and transparent to higher level applications and services. This also includes determination of delivery point(s) of keys.

• Reliable and trustworthy key manager. Whether key managers are centralized or distributed, they should be sufficiently reliable that other entities (including group members) trust them.

(2) Dependent of application

Dependent of application, the essential features that a secure GKMF should have are:

• Secure data exchange. This includes mechanisms for protecting transmitted data, regulating group members' access to data and verifying to any member the nature of the group session in which they participated.

• Group and member authentication. Apart from the initial registration with a trusted group manager upon joining a multicast group, GKMF protocols ought to consider not just verifying that a member is valid and belongs to a valid group (group authentication) but may also choose to verify the actual member (member authentication) participating in the group communication.

4.7.3.2 Desirable features

In this section, independent of application, we identify other desirable but optional features of a GKMF as follows:

- Minimizing computational and storage efforts. Keeping to a minimum the amount of computation that needs to be done, and keys that need to be managed and securely stored, by all communicating entities during a multicast group communication.
- Minimizing traffic implosion. Keeping to a minimum the number of messages that needs to be exchanged during GKMF protocols.
- Reduced trust in third party and intermediate nodes. To minimize the reliance upon third party nodes which may be needed to support a secure GKMF.
- Minimizing risk of attack vulnerabilities. Protecting and minimizing the risk of group data and any keying materials from both passive and active attacks that would compromise the security objectives of the group communication.
- Minimizing risk of colluding members. Minimizing the impact of group members who exchange information in order to gain additional unauthorized access to the group data traffic.
- Coping with system and network failures. Any good and reliable communication architecture should be able to deal with system and network failures, either caused by human errors or natural disasters.

Summary

In this Publications we described the need for multicast functionality has introduced new challenges, particularly with respect to provision of secure environments for such applications. Consequently, the security aspects and security objectives achieved in *unicast* as well as in *broadcast* environments should also be deployed and achieved in multicast environments. We have discussed security issues in group communication and identified several issues specific to this type of environment. Our main interest is in the management of keying material, in particular the distribution and updating of cryptographic keys, which is crucial to ensure the security of any Multicast group communication. We described the basic components of a GKMF and established desirable features which are generic for any networking environments (wired or wireless networks).

REFERENCES

[1]. Rafaeli, S. and Hutchison, D. (2003). A Survey of Key Management for Secure Group Communication. ACM computing Surveys, vol. 35, no. 3, pp. 309-329.

[2]. S. Kamat, S. Parimi, and D. P. Agrawal, "Reduction in control overhead for a secure, scalable framework for mobile multicast," in Communications, 2003. ICC '03. IEEE International Conference on , 2003, pp. 98-103 vol.1.

[3]. S. Mittra, "Iolus: a framework for scalable secure multicasting," SIGCOMM Compute. Common. Rev., vol. 27, pp. 277-288, 1997.

[4]. Wallner, D., E. J. Harder, and Agee, R. (1998). Key Management for Multicast: Issues and Architectures, Internet Draft (work in progress), draft-wallner-key-arch-01.txt, Internet Eng. Task Force.

[5]. Steer, D., Strawczynski, L., Diffie, W., and Wiener, M. (1990). A secure audio teleconference system. In Advances in Cryptology -- CRYPTO'88.

[6]. Chan, H., Perrig, A., and Song, D. (2003). Random Key Pre-distribution Schemes for Sensor Networks. To appear in Proc. Of the IEEE Security and Privacy Symposium.

[7]. Du, W., Deng, J., Han, Y., and Varshney, P. (2003). A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In Proc. of 10th ACM Conference on Computer and Communications Security (CCS), Washington DC.

[8]. Chan, H. and Perrig, A. (2005). PIKE: Peer Intermediaries for Key Establishment in Sensor Networks, In Proceedings of IEEE INFOCOM.

[9]. Chan, A. (2004). Distributed Symmetric Key Management for Mobile Ad hoc Networks, IEEE INFOCOM.

[10]. Shamir, A. (1979). How to Share a Secret. Communications ACM 1979; 22(11), pp. 612–613.

[11]. Wong, T., Wang, C., and Wing, J. (2002). Verifiable Secret Redistribution for Threshold Sharing Schemes. Technical Report, CMU-CS-02-114-R, School of Computer Science, Carnegie Mellon University.

[12]. Stadler, M. (1996). Publicly Verifiable Secret Sharing. Proceeding of Eurocrypt'96. pp. 190-199.

[13]. [13]Luo, H., Zerfos, P., Kong, J., Lu, S., and Zhang, L. (2001). Providing Robust and Ubiquitous Security Support f or Mobile Ad-hoc Networks. Proceeding of The 9th International Conference on Network Protocols.

[14]. Wu, B. and Wu, J. (2007). An Efficient Group Key Management Scheme for Mobile Ad Hoc Networks. Accepted to appear in International Journal of Security and Networks (IJSN).

[15]. P. Judge and M. Ammar, "Security issues and solutions in multicast content distribution: a survey,"Network, IEEE, vol. 17, pp. 30-36, 2003.

[16]. Y. Challal and H. Seba, "Group Key Management Protocols: A Novel Taxonomy. ," Enformatika,

[17]. International Journal of Information technology, vol. 2, 2005.
[18]. J. Bibo and H. Xiulin, "A Survey of Group Key Management," in Computer Science and Software Engineering, 2008 International Conference on , 2008, pp. 994-1002.
[19]. S. Rafaeli and D. Hutchison, " A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, vol. 35, pp. 309 – 329, September 2003 2003.
[20]. I. Romdhani, M. Kellil, L. Hong-Yon, A. Bouabdallah, and H. Bettahar, "IP mobile multicast: Challenges and solutions," Communications Surveys & Tutorials, IEEE, vol. 6, pp. 18-41, 2004.
[21]. C. Perkins, "RFC3344: IP Mobility Support for IPv4,". IETF RFC. Status: Proposed Standard.,August 2002.
[22]. R. Koodli, "RFC5568: Fast Handovers for Mobile IPv6," IETF RFC.Status: Proposed Standard.,July 2009.
[23]. D. Johnson, C. Perkins, and J. Arkko, " RFC3775: Mobility Support in IPv6," IETF RFC. Status: Proposed Standard., June 2004.
[24]. T. Hardjono and L. R. Dondeti, Multicast and Group Security : Artech House, 2003.
[25]. S. Yan, W. Trappe, and K. J. R. Liu, "An efficient key management scheme for secure wireless multicast," in Communications, 2002. ICC 2002. IEEE International Conference on , 2002, pp. 1236-1240 vol.2.
[26]. S. Yan, W. Trappe, and K. J. R. Liu, "Topology-aware key management schemes for wireless multicast," in Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE,2003, pp. 1471-1475 vol.3.
[27]. K. Brown and S. Singh, "RelM:Reliable Multicast for Mobile Networks," Computer Communications,
[28]. vol. 21, pp. 1379-1400, 1998.
[29]. L. Lin, L. Xueming, and C. Yong, "HKM: A Hybrid Key Management Scheme for Secure Mobile Multicast," in Networking, Architecture, and Storage, 2007. NAS 2007. International Conference on, 2007, pp. 109-114.
[30]. C. K. Wong, M. Gouda, and S. S. Lam, "Secure Group Communications Using Key Graphs," ed. ACM SIGCOMM, 1998.
[31]. D. A. McGrew and A. T. Sherman, " Key Establishement in Large Dynamic Groups using One-way Function Trees," Technical Report TR-0755,May 1998.
[32]. W. Yiling, L. Phu Dung, and B. Srinivasan, "Hybrid Group Key Management Scheme for Secure Wireless Multicast," in Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on , 2007, pp. 346-351.
[33]. W. Yiling, L. Phu Dung, and B. Srinivasan, "Efficient Key Management for Secure Wireless Multicast," in
[34]. Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on, 2008, pp. 1131-1136.
[35]. [30] E. Eidkhani, M. Hajyvahabzadeh, S. A. Mortazav, and A. N. Pour, "CRAW: Combination of Re-Keying and Authentication in Wireless Networks for Secure Multicast Increasing Efficiency of Member Join/Leave and Movement,"
[36]. International Journal of Computer Networks & Communications (IJCNC), vol. 4, pp. 107-128, 2012.
[37]. M. Sandirigama, S. Akihiro, and M. Noda, "Simple And Secure password authentication protocol," EICE Trans. Com, vol. E83-B, pp. 1363-1365 2000.
[38]. M. Hajyva299abzadeh, E. Eidkhani, S. A. Mortazavi, and A. N. Pour, "A New Group Key Management Protocol Using Code for Key Calculation: CKC," in Information Science and Applications (ICISA), 2010 International Conference on, 2010, pp. 1-6.
[39]. R. Jong-Hyuk and L. Kyoon-Ha, "Key management scheme for providing the confidentiality in mobile multicast," in Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, 2006, pp. 5 pp.-1209.
[40]. L. R. Dondeti, S. Mukherjee, and A. Samal, "Scalable secure one-to-many group communication using dual encryption," Computer Communications, vol. 23, pp. 1681-1701, 11/1/ 2000.
[41]. C. Ming-Chin and L. Jeng-Farn, "MKMS: Multicast key management scheme for Proxy Mobile IPv6 networks," in Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on , 2011, pp. 1402-1405.
[42]. G. Jianfeng, Z. Huachun, Z. Hongke, and H. Luo, "Multicast Extension Support for Proxy MIPv6," in Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE , 2010, pp. 1-5.
[43]. S.Gundavelli, K. Leung, V. Devarapalli, K.Chowdhury, and B.Patil, "Proxy Mobile IPv6," RFC 5213, August 2008.
[44]. H. Soliman, C. Castelluccia, K. ElMalki, and L.Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility
[45]. Management," RFC 5380, October 2008.
[46]. 2]Burmester, M. and Desmedt, Y. (1994). A Secure and Efficient Conference Key Distribution system. In A. De Santis, editor, Advances in Cryptology – EUROCRYPT '94, no. 950.
[47]. Wong, C., Gouda, M., and Lam, S. (1998). Secure Group Communications Using Key Graphs. In Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication, pp. 68–79.
[48]. B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, et al, "Secure group communications for wireless networks," in Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE , 2001, pp. 113-117 vol.1.